[文章编号] 1003－4684(2026)01-0043-07

基于 Attention-SLSTM 的虚假数据注入攻击检测

王 茹，周先军，张 炎
(湖北工业大学电气与电子工程学院，湖北 武汉 430068)

[摘 要] 针对影响智能电网安全运行问题，提出了一种基于注意力机制的堆叠 LSTM 网络 FDIA 检测方法。堆叠 LSTM 能够通过网络深度增加提取更深层次的特征，而加入注意力机制能够更好的表示模型不同特征层级间的结构关系，增加隐藏层的非线性表达能力，使所提出的模型预测精度更高，从而获得更高的 FDIA 判断准确率。在 IEEE14 节点系统环境下进行验证，实验结果表明，合适层数的 Attention-SLSTM 网络可以获得更高的精确度。与其他几种方法相比，该方法能够取得更好的训练效果，获得更高的 FDIA 检测准确率。

[关键词] 智能电网；虚假数据注入攻击；不良数据检测；堆叠 LSTM 网络；注意力机制
[中图分类号]TP39 [文献标识码] A

电力信息物理融合系统(cyber physical system，CPS)在促进现代电力系统高效配置电力资源、增强其可观测性和可控性的同时，也给现代电力系统通信网络带来了潜在威胁[1-2]。网络安全已成为影响智能电网安全运行的重要因素。虚假数据注入攻击[3](false data injection attack，FDIA)是一种通过篡改量测数据来破坏电网信息完整性的攻击方式，具有较强的可达性、隐蔽性和干扰性，能够绕过传统不良数据检测器的检测，进而影响电网正常运行，直至电力系统停止响应或崩溃。因此，有效检测和抵御 FDIA，确保现代电力系统的稳定安全运行，一直是研究的热点课题。伴随着智能电网的飞速发展，现代电力系统的规模越来越大，数据量呈爆炸式增长，更多专家学者将深度学习应用到智能电网中，来解决各种问题。文献[4]利用电网的拓扑网络图提出了一种图卷积网络框架来检测 FDIA。文献[5]采用改进的图卷积网络对 FDIA 进行检测，并利用变分编码器恢复系统编码器。文献[6]提出一种基于图自编码器和残差网络相结合的模型来检测 FDIA。文献[7]提出了一种基于改进自适应卡尔曼滤波和卷积神经网络的主被动检测方法，以及一种基于 GRU-CNN 模型的主动检测算法。文献[8]提出了一种基于循环神经网络的 FDIA 检测方法，用于实时检测智能电网中的虚假数据注入攻击。

本文针对上述文献未考虑 FDIA 在时序上的检测这一问题，将 FDIA 建模为时序异常检测问题，提出了一种基于 Attention-SLSTM 网络 FDIA 检测机制，采用先预测后判断的方式检测 FDIA。循环神经网络(recurrent neural networks，RNN)能够根据历史测量数据进行预测，从而预防攻击者对电力系统发起的攻击，而 LSTM 可以解决 RNN 在处理超长序列时容易出现“梯度消失”或“梯度爆炸”的现象[9]。采用 Attention-SLSTM 网络模型对历史量测数据进行训练建模，并预测系统产生的未来测量值，计算预测向量与量测向量之间的均方误差(mean square error，MSE)，对比均方误差与预先设定的阈值来检测 FDIA。如果 MSE 超过阈值，模型将判定存在 FDIA。本文所提出的方法不需要标记观测值，且不受噪声环境的影响。

1 问题描述

1.1 状态估计

状态估计是能量管理系统(energy management system，EMS)[10]实现电力系统可靠监测的基本分析工具之一，它根据量测数据和网络拓扑信息估计出系统的真实状态。

电力系统状态估计的形式通常是非线性的。但是在一个稳定运行的电力系统中，假设所有母线的电压幅值相等且为 1，忽略线路的电阻，则测量值中不存在无功功率。因此，电力系统的状态变量与量

[收稿日期] 2024－03－30
[基金项目] 国家自然科学基金(61901165，61601177)；湖北省自然科学基金(2019CFB530)
[第一作者] 王 茹(1998－)，女，河南新乡人，湖北工业大学硕士研究生，研究方向为深度学习、网络安全。
[通信作者] 周先军(1970－)，男，湖北武汉人，湖北工业大学副教授，研究方向为无线网络、移动通信。

测值满足线性关系，直流状态估计可以表示为：

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{e} \tag{1}$$

其中，$\boldsymbol{z}=[z_1,z_2,L,z_m]^{\mathrm{T}}$ 为量测值，主要包括总线电压、有功功率和无功功率；$\boldsymbol{x}=[x_1,x_2,L,x_n]^{\mathrm{T}}$ 为状态向量的集合；$\boldsymbol{e}=[e_1,e_2,L,e_n]^{\mathrm{T}}$ 为量测误差；H 是雅可比矩阵（$\boldsymbol{H}\in R^{m\times n}$），它与网络的拓扑结构有关。

电力系统状态估计问题以冗余的量测值为基础，状态变量的估计值可以通过加权最小二乘法获得，表示为：

$$\hat{x}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}\boldsymbol{z} \tag{2}$$

其中，$\boldsymbol{W}$ 为量测误差的方差组成的对角矩阵。

为了在给定测量中识别不良测量值，提高状态估计结果的可靠性。测量残差的 L_2 范数用于测量实际量测值与正常量测值之间的误差，同时不良数据检测器设置一个特定的阈值 τ_d。因此，可以得出以下不等式：

$$\|\boldsymbol{z}-\boldsymbol{H}[AK\hat{x}]\|\geqslant\tau_d \tag{3}$$

其中，当 $\|\boldsymbol{z}-\boldsymbol{H}\hat{x}\|\geqslant\tau_d$ 时，则这些量测值被怀疑为不良量测值。否则，当 $\|\boldsymbol{z}-\boldsymbol{H}\hat{x}\|<\tau_d$ 时，采集到量测值为正常数据。

1.2 虚假数据注入攻击建模

FDIA 是以破坏电网信息完整性为目的，专门针对电力系统状态估计环节发起的一种新型网络攻击。其通过向传感器等智能仪表与数据采集监控系统（supervisory control and dataacquisition，SCADA）之间的通信网络注入攻击向量或以 SCADA 为媒介的方式恶意篡改 EMS 接收的量测数据，使得控制中心得到的估计结果不真实，误判系统当前所处的状态，造成系统安全措施被动或拒动，最终影响电力系统的稳定运行[11]。假设当攻击者完全了解电网的拓扑结构信息时，便可利用不良数据检测（Bad Data Detection，BDD）方法的缺陷，对电网进行 FDIA。当电网受到攻击时，受到 FDIA 后的量测值

$$z_a=z+a \tag{4}$$

其中，$\boldsymbol{a}=[a_1,a_2,\cdots,a_m]^{\mathrm{T}}$ 为注入的攻击向量。

于是，受到攻击后的状态估计值 $\hat{x}_a$ 可表示为：

$$\hat{x}_a=(H^{\mathrm{T}}W^{-1}H)^{-1}H^{\mathrm{T}}W^{-1}z_a=\hat{x}+c \tag{5}$$

其中，$\boldsymbol{c}$ 为攻击后状态向量中引入的误差向量。

此外，测量残差的 L_2 可以表示为：

$$\begin{aligned}&\|z_a-H\hat{x}_a\|=\|z+a-H(\hat{x}+c)\|=\\&\|z-H\hat{x}+a-Hc\|=\|z-H\hat{x}\|\end{aligned} \tag{6}$$

其中，当 $a=Hc$ 时，受攻击前后的残差一致，FDIA 可成功地绕过 BDD，且不易被发现。

2 基于 Attention-SLSTM 的 FDIA 检测方案

2.1 LSTM 网络

LSTM[12] 是循环神经网络 RNN 的一种改进版本，能够处理长距离的依赖问题。在 LSTM 中，引入了门控机制，当输入序列较长时，通过门控制将短期记忆与长期记忆结合起来，在一定程度上能够避免“梯度消失”或“梯度爆炸”现象[13]。LSTM 的结构单元如图 1 所示。

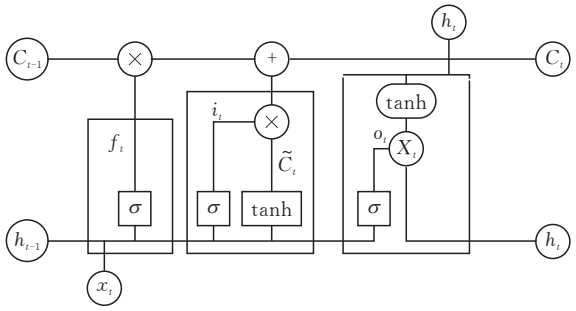

图 1 LSTM 单元结构

LSTM 由遗忘门、记忆门和输出门组成，控制信息的保留和传递，最终得到细胞状态 C_t 和输出信号 h_t。遗忘门的任务是接收上一个时刻的输出信号 h_{t-1} 和 t 时刻的输入信号 x_t，通过 sigmoid 型函数决定保留和遗忘 C_{t-1} 的某个部分。遗忘门的输出值

$$f_t=\sigma(\boldsymbol{w}_f[x_t,h_{t-1}]+\boldsymbol{b}_f) \tag{7}$$

其中，f_t 的值介于 0 和 1 之间；$\boldsymbol{b}_f$ 为偏置矢量；$\boldsymbol{w}_f$ 权重向量。

记忆门与遗忘门的作用相反，它接收与遗忘门一样的输入，第一部分是通过 sigmoid 型函数会输出一个介于 0 到 1 之间的数值：

$$i_t=\sigma(w_i[x_t,h_{t-1}]+b_i) \tag{8}$$

其中，w_i、b_i 分别为 sigmoid 型函数的权重和偏置。

第二部分是将输入通过 tanh 型函数创建为一个新的候选状态向量：

$$\tilde{\boldsymbol{C}}_t=\tanh(w_c[x_t,h_{t-1}]+b_c) \tag{9}$$

其中，w_c、b_c 分别为 tanh 型函数的权重和偏置。

因此遗忘门和记忆门可以将细胞状态更新为：

$$C_t=f_tC_{t-1}+i_t\tilde{C}_t \tag{10}$$

输出门是输出当前时刻的输出信号 h_t，并作为下一时刻的输入信号，可表示为：

$$o_t=\sigma(w[x_t,h_{t-1}]+b_t) \tag{11}$$

$$h_t=\tanh(C_t)o_t \tag{12}$$

2.2 堆叠 LSTM 网络

单层的神经网络对数据特征提取的能力较弱，同时表达能力略显不足。而采用堆叠 LSTM 网络，通过增加网络的深度，不仅能够提高网络模型的训

练效率，也能够获得更高的预测准确性，使得堆叠 LSTM 网络成为处理序列预测问题的成熟技术之一。堆叠 LSTM 网络[14]结构可以定义为由多个 LSTM 隐藏层组成的 LSTM 网络模型。在每一个时刻，堆叠 LSTM 网络的每个输入序列分别对应一个输出序列，通过加深网络的深度来延长数据特征提取的时间。因此，在处理和分析序列数据时，堆叠 LSTM 网络能够提高序列问题预测的精度。

2.3　注意力机制

注意力机制(attention mechanism)源于对人类视觉的研究[15]。在认知科学中，人类会有选择性地关注一些重要的信息，而忽视那些不重要且无关的信息。注意力机制是解决信息超载问题的一种主要手段，即将资源进行分配的一种方案，并决定将资源分配给重要的部分[16]。注意力机制的作用主要包含两个方面：一是计算输入项权重，决定关注的重要部分是哪些；二是将有限的信息资源分配给关键的决定性部分。神经网络中的注意力机制是以端到端的目标导向方式进行学习的，是一种自上而下的注意力。注意力机制对模型中各类不同的元素赋予了各自不同的权重，对于重要的影响参数，对其权重进行增加，对于不相关的信息，将权重进行缩减[17]。这有助于进一步降低模型的运算复杂度，将分类模型的关注重点集中在重要的参数部分。

2.4　基于 Attention-SLSTM 网络 FDIA 检测模型

FDIA 检测问题可以建模为时间序列异常检测问题，采用先预测后判断的思路进行检测。RNN 在时间序列预测方面具有一定的优势，但其在处理超长序列时容易出现梯度消失与梯度爆炸的问题，而 LSTM 能够缓解这种问题。因此，本文提出了基于注意力机制的堆叠 LSTM 网络 FDIA 检测模型。堆叠 LSTM 能够对长序列数据进行高维时间的特征提取，加入注意力机制可以增强模型的非线性表达能力。基于 Attention-SLSTM 的 FDIA 检测模型如图 2 所示，其中模型主要包含一个输入层、多个堆叠 LSTM 层、多个注意力层和一个输出层。

1)输入层　攻击者从系统状态估计中得到雅可比矩阵、误差向量和状态向量，然后设置一定百分比的攻击向量绕过 BDD 到达控制中心。通过公式(4)得到量测向量。由于数据集是实值且具有时间连续型，本文采用数据窗口来处理数据，以生成时间序列数据用于堆叠 LSTM 网络模型的训练。本文设置窗口大小为 6，其中输入宽度为 5，输入宽度决定有多少输入注入到模型中。

2)堆叠 LSTM 层　在本文所提出的 FDIA 检测模型中，采用堆叠 LSTM 作为隐藏层，多个

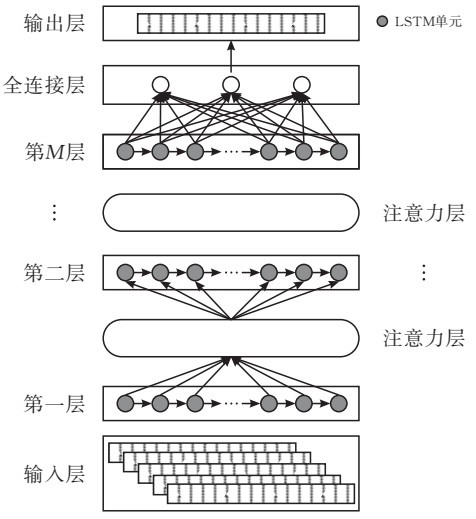

图 2　基于注意力机制的堆叠 LSTM 网络 FDIA 检测方案

LSTM 单元逐层提取数据特征，上一个 LSTM 单元的输出作为下一个 LSTM 单元的输入。其中，堆叠 LSTM 网络在较低层提取基本概念特征，高层的 LSTM 单元提取更深更高维的时间特征，其优势在于能够延长时间序列数据的特征提取时间。

3)注意力机制层　注意力层在堆叠 LSTM 隐藏层之后，它对堆叠 LSTM 提取的时间特征进行加权求和，提取样本数据间的深层次特征，增强特征的非线性表达能力，进而提高堆叠 LSTM 对数据的预测精度。注意力机制层的展开形式如图 3 所示。

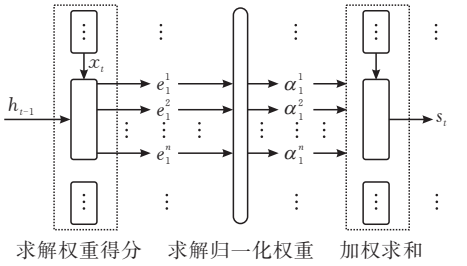

图 3　注意力机制结构

第一步求解权重得分，权重即特征向量对模型识别的贡献大小，其计算方法为：

$$e^t = v^{\mathrm{T}} \cdot \tanh(\boldsymbol{W}_a \cdot \boldsymbol{x}_t + b) \tag{13}$$

其中，v^{T} 和 b 均为超参数；$\boldsymbol{W}_a$ 为注意力矩阵[18]，需要随机初始化设置；$\boldsymbol{x}_t$ 为输入向量；维度为 $n \times m$，n 表示模型批量处理的样本数，m 为 LSTM 隐藏层神经元的个数。输入向量为 LSTM 的隐藏层状态 H_t 或者单元状态 C_t，即

$$H_t = (h_t^{(1)}, h_t^{(2)}, \ldots, h_t^{(l)}) \tag{14}$$

$$C_t = (c_t^{(1)}, c_t^{(2)}, \ldots, c_t^{(l)}) \tag{15}$$

其中，$h_t^{(l)}$ 和 $c_t^{(l)}$ 分别代表在第 t 个时间步上的 l 层 LSTM 单元隐藏层的状态以及单元状态。

第二步求解归一化权重，其加权系数为：

$$\alpha^t = \frac{\exp(e_j^t)}{\sum_{j=1}^{T}\exp(e_j^t)} \tag{16}$$

其中，e_j^t 表示第 j 个元素的权重得分；T 表示为总的时间步长。

第三步求解加权和：

$$s^t = \sum_{j=1}^{T}\alpha_j^t x_{tj} \tag{17}$$

其中，α_j^t 表示第 j 个元素的加权系数；$\boldsymbol{x}_{tj}$ 表示第 j 个输入向量。

4)输出层　FDIA 检测模型输出前有一个全连接层，使其从一个特征空间线性变换到另一个特征空间以便进行输出。数据窗口的标签宽度设置为 1，标签宽度即模型的输出，也就是预测向量。

基于注意力机制的堆叠 LSTM 网络模型检测 FDIA 的原理是：首先对 FDIA 是否存在进行预测，然后根据设定的阈值进行判断。计算测量向量与预测向量之间的 MSE 值，将 MSE 值与预先设定的阈值进行比较。如果包含攻击数据的测量向量与预测向量之间的 MSE 值超过设定阈值，则模型可以检测到 FDIA 存在；否则，模型未检测到 FDIA，即不存在 FDIA。MSE 可以表示为：

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{m} w_i\,(y_i - \hat{y}_i)^2 \tag{18}$$

其中，y_i 是真实数据；$\hat{y}_i$ 是预测数据；$w_i > 0$；n 为样本的个数。

3　实验结果与分析

3.1　数据集及预处理

本文提出的基于注意力机制的堆叠 LSTM 的虚假数据检测需要大量的历史数据，结合实际情况，决定采用 IHEPCDS 数据集，即一个法国家庭连续四年的真实用电负荷数据。该数据集监测持续时间最长，包含 100 多万个数据点。对数据集进行分析和处理后，使其能够满足训练、测试和验证所需的指标要求，例如连续时间、实际功率流等。首先对数据集进行清理，存在缺失或明显错误的数据条目在经过状态估计后会被不良数据检测剔除。然后，对数据集在不同时间段的能源负荷进行数据分析，提取数据集中的潜在模式，生成所需的全局功率流数据集，同时生成的有功功率和无功功率必须强制使用 float 数据类型。如图 4 所示，它是所生成的正常数据集的一个分支有功功率流。

为了更好地模拟智能电网运行环境，本文以 IEEE14 节点测试系统作为测试环境，其系统结构如图 5 所示。为了复现 IEEE14 节点系统的原始行为，将编号为 1、7、8 的总线设为零值，其余的 11 个负荷节点分别作为 11 个区域代表。

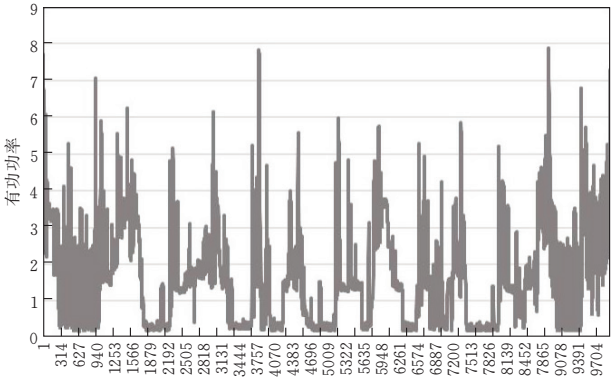

图 4　正常数据的一个分支功率流

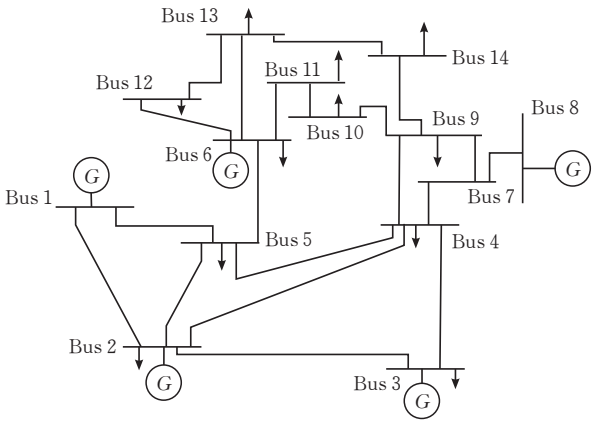

图 5　IEEE 14 节点系统结构

在 IEEE14 节点系统中，通过 MATPOWER 进行潮流分析，潮流分析采用有功功率和无功功率注入，这有助于从中提取真实的功率流，生成的 25 个测量值作为实验中的观察值，主要包含 14 列有功功率注入和 11 列实际功率流。在状态估计过程中，其目标是获取发动攻击所需要的两个要素，即雅可比矩阵和误差向量。在收集雅可比矩阵、误差向量和测量向量后，通过公式 $a = Hc$，攻击者可以根据雅可比矩阵的维数伪造可以绕过不良数据检测器的攻击数据。本文生成的数据集中，正常数据和受损数据的对比关系如图 6 所示。

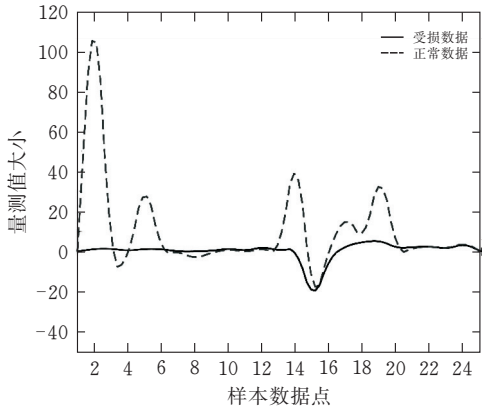

图 6　攻击前后数据对比

在表 1 中，本文展示了实验中所使用的生成数据集的统计数据。通过实验发现，模型训练的数据点越多，其模型精度越高。本文对 100 多万条数据进行处理后，选择了其中无时间缺失的最长连续时间样本，总计采用了 6 万多条数据。其中，选取无攻击向量数据的 70%作为训练集和验证集，30%作为测试集评估预测模型性能。

表 1　数据统计

数据集	正常数据	异常数据	总数
训练集和验证集	47037	0	47037
测试集	16495	3663	20158

3.2　评价指标

本文在处理数据集的过程中，对正常数据和攻击数据分别添加标签，0 表示正常数据，1 表示攻击数据。因此，对于实验模型的评估采用准确率、精确率、召回率和 $F1$ 值这四个评价指标。假设遭受攻击的数据为正，正常状态的数据为负。如表 2 的混肴矩阵所示，TP 为被模型预测为正的正样本，TN 为被模型预测为负的负样本，FP 为被模型预测为正的负样本，FN 为被模型预测为负的正样本。

表 2　二分类的混淆矩阵

		实际结果	
		1	0
预测结果	1	TP	FP
	0	FN	TN

准确率为预测正确的结果占总样本的百分比，其定义如下：

$$A_c = \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \tag{19}$$

精确率为预测为正样本的数据占实际正样本的概率

$$P = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \tag{20}$$

召回率是实际为正的样本中被预测为正样本的概率

$$R = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{21}$$

$F1$ 值为精确率和召回率的调和平均数：

$$F1 = \frac{2PR}{P+R} = \frac{2\mathrm{TP}}{2\mathrm{TP}+\mathrm{FN}+\mathrm{FP}} \tag{22}$$

3.3　实验环境与性能分析

本文实验使用 Python 作为编程语言，开发工具为 Pycharm，深度学习框架为 Tensorflow。堆叠 LSTM 参数设置如下：批处理大小 batch_size 为 15，最大 epoch 为 20，采用 Rmsprop 作为优化算法，初始学习率设置为 0.0001，神经元数量为 64，全连接层单元数为 25。为了防止在训练中出现过拟合，分别在每个堆叠 LSTM 层之间和最后一层堆叠 LSTM 与全连接层之间加入了 Dropout 层，丢弃概率为 20%。

为了验证本文所提方法的有效性，对比不同算法的 FDIA 检测结果，如表 3 所示。对比的四种算法均是在它们各自 FDIA 检测中的最高准确率。因为正负样本数据的比例存在不平衡性，有时准确率并不能作为很好的评价指标来衡量结果，所以将 $F1$ 值也作为检测 FDIA 模型性能的评价指标。实验结果表明，所提出基于 Attention-SLSTM 网络的 FDIA 检测模型，其准确率和 $F1$ 值均可以得到最高值，其模型性能和效果是所有方法中最优的。这是因为多个堆叠 LSTM 层的叠加增加了模型的网络深度，有助于延长序列数据特征提取的时间，从而获得更高的精度。同时，注意力机制通过对堆叠 LSTM 网络的输出特征进行加权分配，对数据间或数据中的特征注入更多关注，增强堆叠 LSTM 的非线性表达能力，提升其预测精度。

表 3　不同模型的实验结果对比

方法	A_c	P	R	$F1$
LSTM	0.982	1.0	0.904	0.95
CNN	0.886	0.575	0.994	0.728
SVM	0.863	0.571	0.99	0.726
Attention-SLSTM	0.994	0.987	1.0	0.993

另外，表 4 为堆叠 LSTM、LSTM、CNN 和 SVM 四种预测模型的均方根误差（root mean square error，RMSE）以及训练时间的对比。均方根误差是真实值与预测值之间的偏差，对数据中的异常值非常敏感。由表 4 可以看出，本文所提出的基于 Attention-SLSTM 网络 FDIA 检测模型的均方根误差均小于其他三种预测模型，加入注意力机制可以增强堆叠 LSTM 网络的特征提取能力，使其预测性能优于其他网络模型。另外，从训练时间上看，本文所提出的 FDIA 检测模型的训练时间高于 CNN 与 SVM 两种预测模型。原因是 CNN 与 SVM 网络的结构比较简单，而堆叠 LSTM 的网络深度较深，延长了特征提取的时间。

表 4　不同模型的性能结果对比

方法	训练集 RMSE	测试集 RMSE	训练时间/s
LSTM	1.45	1.66	424
CNN	1.49	1.68	105
SVM	1.56	1.75	101
Attention-SLSTM	1.16	1.54	387

为了研究隐藏层层数对所提出 FDIA 检测模型性能的影响，分别采用具有 1～5 层隐藏层的堆叠 LSTM 网络来训练并测试，其中每个隐藏层之后都含有一个注意力机制层，每个隐藏层分别有 64 个单

元。如图 7 所示，可以发现隐藏层的层数是影响算法性能的关键因素之一。随着隐藏层数量的增加，检测 FIDA 的准确率和 $F1$ 值都是先上升后下降。当堆叠层数为 3－4 层时，可以取得较高的检测率，即如果网络层数太浅，则无法提取足够的特征来进行准确预测。但当层数达到 5 层时，其检测率比单层的还要低，这说明当网络层数过深时，层与层之间的梯度消失情况会非常明显，收敛效果和训练效率都会大幅下降，进而使得算法性能下降。因此，合适的网络层数可以提升模型的性能，并不是网络层数越深越好。

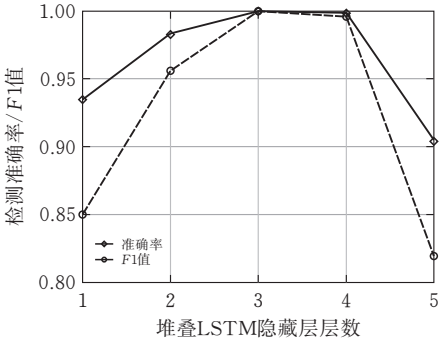

图 7 不同隐藏层数下所提方案的性能

4 结论

本文针对电力系统中隐蔽的 FDIA 不易被检测到的问题，将其建模为时序异常检测问题，提出了一种基于 Attention-SLSTM 网络 FDIA 检测机制。堆叠 LSTM 网络作为特征提取层来提取样本数据的深层次特征，同时加入注意力机制计算数据权重合理分配资源，增加隐藏层的非线性表达能力，使所提出的 Attention-SLSTM 网络模型预测精度更高且具有鲁棒性，从而提高了 FDIA 的检测准确率。实验结果表明，与其他方法相比，所提出的 Attention-SLSTM 网络模型检测 FDIA 的准确率更高，且模型预测性能更优，能够更有效地防范 FDIA，维护电力系统平稳安全运行。

[参 考 文 献]

[1] 李士达. 基于 SCADA 系统的铁路工程及其在设备故障诊断中的研究与应用[D]. 北京：华北电力大学，2014.

[2] VELLAITHURAI C，SRIVASTAVA A，ZONOUZ S，et al. CPIndex：Cyber-physical Vulnerability Assessment for Power-grid Infrastructures[J]. IEEE Transactions on Smart Grid，2014，6(02)：566-575.

[3] LIU Y，NING P，REITER M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security(TISSEC)，2011，14(01) ：309-341.

[4] VINCENT E，KORKI M，SEYEDMAHMOUDIAN M，et al. Detection of false data injection attacks in cyber-physical systems using graph convolutional network[J]. Electric Power Systems Research，2023，217：109118.

[5] 陈柏任，夏候凯顺，李梦诗. 基于数据驱动的电力系统虚假数据注入攻击防御框架的研究[J/OL]. 电测与仪表：1-9[2022-06-28]. http：//kns.cnki.net/kcms/detail/23.1202.TH.20220518.1541.006.html.

[6] WANG Y，ZHANG Z，MA J，et al. KFRNN：an effective false data injection attack detection in smart grid based on kalman filter and recurrent neural network[J]. IEEE Internet of Things Journal，2021，9(09)：6893-6904.

[7] QU Zhaoyang，BO Xiaoyong，YU Tong，et al. Active and passive hybrid detection method for power CPS false data injection attacks with improved AKF and GRUCNN[J]. IET Renewable Power Generation，2022，16：1490-1508.

[8] JAFARI A，ERGUN H，VAN HERTEM D. A Voting-Based Machine Learning Strategy to Detect False Data Injection Attack in Cyber-Physical Power Systems[C]// 2022 57th International Universities Power Engineering Conference (UPEC). IEEE，2022：1-6.

[9] 陈礼贤，梁杰，黄一帆，等. 基于深度自回归循环神经网络的边缘负载预测[J]. 小型微型计算机系统，2024，45(02)：359-366.

[10] 田继伟，王布宏，尚福特. 基于鲁棒主成分分析的智能电网虚假数据注入攻击[J]. 计算机应用，2017，37(07)：1943-1947.

[11] 吴迪. 虚假数据攻击下电力系统安全检测技术研究[D]. 秦皇岛：燕山大学，2020.

[12] SHERRATT F，PLUMMER A，IRAVANI P. Understanding LSTM network behaviour of IMU-based locomotion mode recognition for applications in prostheses and wearables[J]. Sensors，2021，21(04)：1264.

[13] 卢强，朱振方，徐富永，等. 融合语法规则的 Bi-LSTM 中文情感分类方法研究[J]. 数据分析与知识发现，2019，3(11)：99-107.

[14] 刘建伟，宋志妍. 循环神经网络研究综述[J]. 控制与决策，2022，37(11)：2753-2768.

[15] 代翔. 基于注意力循环网络的 4D 轨迹预测模型[J]. 电讯技术，2022，62(01)：39-45.

[16] KOSIOREK A. 神经网络中的注意力机制[J]. 机器人产业，2017，6：14.

[17] 谭庆康，潘沛生. 基于注意力机制的堆叠 LSTM 心电预测算法[J]. 计算机技术与发展，2023，33(01)：62-67.

[18] 张一凡，张双辉，刘永祥，等. 基于注意力机制的堆叠 LSTM 网络雷达 HRRP 序列目标识别方法[J]. 系统工程与电子技术，2021，43(10)：2775-2781.

False Data Injection Attack Detection Based on Attention-SLSTM

WANG Ru,ZHOU Xianjun,ZHANG Yan

(*School of Electrical and Electronic Engineering, Hubei Univ. of Tech., Wuhan* 430068, *China*)

Abstract: False Data Injection Attack (FDIA) has strong interference, concealment and accessibility, and can easily bypass bad data detectors to affect the safe operation of smart grid. From the perspective of time series anomaly detection, an Attention Stacked Long Short Term Memory (Attention-SLSTM) FDIA detection method based on attention mechanism is proposed by adopting the detection idea of "prediction first, then judgment". Stacked LSTM can extract deeper features by increasing the depth of the network, and adding attention mechanism can better represent the structural relationship between different feature levels of the model, increase the nonlinear expression ability of the hidden layer, and make the proposed model prediction accuracy higher, so as to obtain higher accuracy for determining whether FDIA exists. Verified in the IEEE14 nodes system environment, experimental results show that the Attention-SLSTM network with the appropriate number of layers can achieve higher accuracy. Compared with several other methods, it can achieve better training results and obtain higher FDIA detection accuracy.

Keywords: smart grid; false data injection attacks; bad data detected; stacked LSTM networks; attention mechanism

[责任编校: 赵　瞳]

(上接第 36 页)

Fault Feature Extraction of Distribution Network Based on ISSA-VMD Singular Entropy

LI Shulin, SONG Haoran, ZHAO Guo

(1 *Hubei Key Laboratory for High-efficiency Utilization of Solar Energy and Operation Control of Energy Storage System, Hubei Univ. of Tech., Wuhan* 430068, *China*)

Abstract: Aiming at the non-linearity and non-stationarity of distribution network fault signals, and the traditional time domain analysis method and frequency domain analysis method can no longer meet the problem of distribution line fault type identification. A distribution network fault feature extraction based on ISSA-VMD singular entropy is proposed. Since the number of mode decomposition K and penalty factor α of variational mode decomposition affect the result of signal decomposition, the improved sparrow algorithm is used to optimize the parameters, and then the ISSA-VMD algorithm is combined with Tsallis singular entropy to complete the extraction of fault signal features and construct fault feature vectors. Experiments show that it can effectively distinguish four types of fault types, such as single-phase grounding, two-phase grounding, two-phase short circuit and three-phase short circuit, and distinguish the fault types according to the voltage singular entropy or current singular entropy between phases, so as to distinguish 10 fault types.

Keywords: distribution network fault signal, variational mode decomposition, sparrow algorithm, singular entropy

[责任编校: 赵　瞳]